## CLAIMS

1. An encrypted communication system comprising a first device and a second device, wherein

the first device (i) encrypts a 1st key using a public key of the second device to generate 1st encrypted data, and transmits the 1st encrypted data to the second device, (ii) receives 2nd encrypted data from the second device, and decrypts the 2nd encrypted data using a secret key of the first device to obtain a 2nd key, and (iii) generates, based on the 1st and 2nd keys, a 1st encryption key for use in communication with the second device,

the second device (i) encrypts a 3rd key using a public key of the first device to generate the 2nd encrypted data, and transmits the 2nd encrypted data to the first device, (ii) receives the 1st encrypted data from the first device, and decrypts the 1st encrypted data using a secret key of the second device to obtain a 4th key, and (iii) generates, based on the 3rd and 4th keys, a 2nd encryption key for use in communication with the first device, and

the first and second devices perform encrypted communication using the 1st and 2nd encryption keys.

2. A communication device for performing encrypted

communication with another device using a shared key, comprising:

a data generation unit operable to encrypt a 1st key using a public key that corresponds to a secret key held by the other device to generate 1st encrypted key data, and transmit the 1st encrypted key data to the other device;

a decryption unit operable to receive, from the other device, 2nd encrypted key data generated by the other device encrypting a 3rd key using a public key of the communication device, and decrypt the 2nd encrypted key data using a secret key of the communication device to obtain a 2nd key;

a key generation unit operable to generate an encryption key based on the 1st and 2nd keys; and

a communication unit operable to perform encrypted communication with the other device using the encryption key.

3. The communication device of claim 2, wherein

the key generation unit further generates a hash key based on the 1st and 2nd keys, and

the communication unit includes:

a calculation subunit operable to calculate, using the hash key, a hash value for transmission data;

an encryption subunit operable to encrypt the transmission data using the encryption key to generate

encrypted data; and

a transmission subunit operable to transmit the hash value and the encrypted data to the other device.

4. The communication device of claim 3, wherein the key generation unit concatenates the 1st and 2nd keys to generate concatenated data, calculates a hash value for the concatenated data, and generates the encryption key and the hash key based on the hash value.

5. The communication device of claim 3, wherein the key generation unit performs an exclusive OR operation using the 1st and 2nd keys, and generates the encryption key and the hash key based on a result of the operation.

6. The communication device of claim 2, wherein

the key generation unit further generates a hash key based on the 1st and 2nd keys,

the communication unit includes:

a receiving subunit operable to receive, from the other device, encrypted data generated by encrypting data using an encryption key held by the other device, and a 1st hash value calculated for the data using a hash key held by the other device;

a decryption subunit operable to decrypt the encrypted data using the encryption key to obtain plaintext data; and

a judging subunit operable to calculate a 2nd hash value for the plaintext data using the hash key, and judge whether the first and second hash values match, and

the communication device further includes a usage unit operable to use the plaintext data if the hash values are judged to match, and to suppress use of the plaintext data if the hash values are judged not to match.

7. The communication device of claim 2 further comprising an authentication unit operable to authenticate the other device, using the encryption key.

8. The communication device of claim 7, wherein

the authentication unit (i) generates a 1st authentication value, encrypts the 1st authentication value using the encryption key to generate a 1st encrypted value, and transmits the 1st encrypted value to the other device, and (ii) receives, from the other device, a 2nd authentication value generated by decrypting the 1st encrypted value using an encryption key held by the other device, and judges whether the 1st and 2nd authentication values match, and

the communication device further comprises a communication unit operable to perform communication with the other device if the authentication values are judged to match.

9. The communication device of claim 8, wherein

the authentication unit receives, from the other device, a 3rd encrypted value generated by encrypting a 3rd authentication value using the encryption key held by the other device, decrypts the 3rd encrypted value using the encryption key to obtain a 4th authentication value, and transmits the 4th authentication value to the other device, and

the communication unit performs the communication if the other device judges the 3rd and 4th authentication values to match.

10. The communication device of claim 2, wherein

the data generation unit encrypts the 1st key based on a key encapsulation mechanism to generate the 1st encrypted key data, and

the decryption unit decrypts the 2nd encrypted key data based on a key decryption mechanism to obtain the 2nd key.

11. A method used by a communication device that performs encrypted communication with another device using a shared key, comprising the steps of:

encrypting a 1st key using a public key that corresponds to a secret key held by the other device to generate 1st encrypted key data, and transmitting the 1st encrypted key data to the other device;

receiving, from the other device, 2nd encrypted key data generated by the other device encrypting a 3rd key using a public key of the communication device, and decrypting the 2nd encrypted key data using a secret key of the communication device to obtain a 2nd key;

generating an encryption key based on the 1st and 2nd keys; and

performing encrypted communication with the other device using the encryption key.

12. A computer program used by a communication device that performs encrypted communication with another device using a shared key, the computer program causing a computer to execute the steps of:

encrypting a 1st key using a public key that corresponds to a secret key held by the other device to generate 1st encrypted key data, and transmitting the 1st encrypted key

data to the other device;

receiving, from the other device, 2nd encrypted key data generated by the other device encrypting a 3rd key using a public key of the communication device, and decrypting the 2nd encrypted key data using a secret key of the communication device to obtain a 2nd key;

generating an encryption key based on the 1st and 2nd keys; and

performing encrypted communication with the other device using the encryption key.

13. A computer-readable recording device storing a computer program used by a communication device that performs encrypted communication with another device using a shared key, the computer program causing a computer to execute the steps of:

encrypting a 1st key using a public key that corresponds to a secret key held by the other device to generate 1st encrypted key data, and transmitting the 1st encrypted key data to the other device;

receiving, from the other device, 2nd encrypted key data generated by the other device encrypting a 3rd key using a public key of the communication device, and decrypting the 2nd encrypted key data using a secret key of the communication

device to obtain a 2nd key;

generating an encryption key based on the 1st and 2nd keys; and

performing encrypted communication with the other device using the encryption key.